KDT750
Price Verification System

User's Guide

Effective date: **April 2009**

Revision History

November 11, 2008 – Initial version

November 25, 2008 – Merge Integration Guide and User's Manual

December 1, 2008 – Minor punctuation fixes and additions, better unit introduction, add wireless network diagram, remove MT7570 reference in Appendix B

April 9, 2009 – Updated to include KDT750 Setup Utility. Remove references to manual settings file editing. Add information on updated boot procedure and User Applications.

© 2009 American Microsystems, Ltd. All rights reserved.

American Microsystems, Ltd. reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult American Microsystems, Ltd. to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of American Microsystems, Ltd.

American Microsystems, Ltd. shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

This document contains proprietary information which is protected by copyright.

All rights are reserved. No part of this document may be photocopied, reproduced or translated into another language without the prior written consent of American Microsystems, Ltd.

American Microsystems, Ltd.
2190 Regal Parkway • Euless, TX 76040
Phone 800.648.4452 • Fax 817.685.6232
www.amltd.com

Table of Contents

About This Document
Introduction
What to Expect
Chapter Descriptions
Related Documents

Chapter 1 – Introduction
Introducing the KDT750
Part Numbers and Model Information
Warranty Information
Agency Compliance

Chapter 2 – Getting Started
KDT750 Startup Sequence
Entering System Setup
Navigating Setup
Changing the User Boot Application

Chapter 3 – Terminal Overview
Outer Case Description
Rear Panel Description
Opening the KDT750 Outer Case
Internal Connections
Internal Connector Pinouts
External Connections
Wiring Installation
Power Requirements and Battery Information
Main Power Switch and Power-On Reset
Secure Digital (SD) Card

Chapter 4 – Communications and Input
Network Communications
Serial Communications
USB Communications
Digital I/O
Weigand Interface
Software Keyboard Wedge
Pushbutton Input

Chapter 5 – Wireless Networking
Overview
802.11 Fallback
Interference and Coexistence
Encryption and Authorization
Wireless Configuration
Wireless Network Parameters
Example Configurations

Chapter 6 – Integrated Bar Code Scanner
Overview
Determining Scanner Type
Linear CCD Aiming System and Decode Zones
2D Omni Scanner Aiming System and Decode Zones
Triggering the Scanner
Scanning Bar Codes
Supported Bar Code Symbologies
Obtaining and Using Scan Engine Setup Bar Codes

Chapter 7 – Installed Software
PCDemo
KDT750 Demo
Bar Code Data Viewer
Links2 Web Browser
On-Screen Keyboard
VT100.220 Terminal Emulator

Chapter 8 – Mechanical Integration and Mounting
Rear Panel Mount Points
Flush Wall Mounting
Angled Wall Mounting
Column/Post Mounting
RAM Mounts

Appendix A – Technical Specifications
Appendix B – Wireless Reference Table

About this Document

Introduction

This document describes the integration and general use of the AML KDT750 price verification terminal.

This document is provided as **PRELIMINARY ONLY** and is not intended as a complete product reference. AML reserves the right to make changes to this document and to any hardware, software or product it describes.

What to Expect

This user's guide provides an overall physical description, built-in hardware functions, technical specifications and performance capabilities of the KDT750 terminal. In addition you will learn how to:

- Open the tamper resistant case
- Connect communication cables
- Cold boot and warm reset the KDT750
- Navigate the KDT750 software
- Mount the unit using optional accessories

Chapter Descriptions

Chapter 1 – gives a brief overview of the KDT750, its product warranty and agency compliance

Chapter 2 – gives a quick start introduction to the KDT750 unit

Chapter 3 – describes the KDT750 terminal hardware and details internal and external cable connections

Chapter 4 – describes the communication and user input capabilities of the KDT750

Chapter 5 – describes the use and configuration of the optional 802.11 wireless LAN radio

Chapter 6 – describes the use of the optional internal bar code scanner

Chapter 7 – describes the KDT750's preinstalled software suite

Chapter 8 – describes methods to mount the KDT750 unit in a variety of environments

Related Documents

KDT750 – APL: AML Price Lookup Protocol, Revision 20081106BMC

1

Introduction

This chapter gives a brief overview of the KDT750, it's product warranty and agency compliance.

Introducing the KDT750

The KDT750 is an industrially rated, kiosk-style data terminal designed for use in retail price checking, retail data collection, real-time work-in-process, industrial data collection, consumer lookup and time and attendance.

The terminal is designed around a 5.6" Full VGA, high-color LCD with integrated touch-screen that provides an unsurpassed viewing experience. The ultra-bright LED backlight allows for viewing images and text on the screen in even the brightest of environments.

The KDT750 is designed to be connected to multiple external and internal data sources including bar code scanners, magnetic stripe readers, keyboards, proximity card readers and other modern information collection devices. Its primary wide area communication is through an integrated Power-over-Ethernet ready 10/100 BaseTX Ethernet port or an optional 802.11b/g/n radio.

With a dual port digital I/O and 3 full-speed USB host ports, the KDT750 can be adapted into any environment and provides a cost-effective solution for any number of industrial and consumer installations.

Part Numbers and Model Information

Model Number	Bar Code Scanner	Wired Networking	Wireless Networking	Backup Battery	Power-over-Ethernet
KDT750-0000	n/a	10/100 BaseTX	n/a	n/a	802.3af
KDT750-0001	CCD	10/100 BaseTX	n/a	n/a	802.3af
KDT750-0002	2D	10/100 BaseTX	n/a	n/a	802.3af
KDT750-0010	n/a	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT750-0011	CCD	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT750-0012	2D	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT750-0100	n/a	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT750-0101	CCD	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT750-0102	2D	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT750-0110	n/a	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT750-0111	CCD	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT750-0112	2D	10/100 BaseTX	802.11b/g	2200 mAh	802.3af

CCD = Linear Imager
2D = Omni-directional Imager with 2-Dimensional decoding

Part Number	Description
ACC-0750	KDT750 Pole/Post Mount Kit
ACC-0752	KDT750 Angled Wall Mount Kit
ACC-0754	KDT750 Ram Mount Kit
ACC-750MSR	KDT750 Magnetic Stripe Reader Kit (Top Mount)
ACC-750HID	KDT750 HID ProxPoint Plus Reader Kit (Side Mount)

Warranty Information

A one-year warranty against material defects and workmanship from the date of shipment is guaranteed by AML. Products are sold on the basis of specifications applicable at the time of manufacture. AML shall have no obligation to modify or update products once sold. At our option, we will repair or replace, at no charge, any unit that proves to be defective providing the appropriate steps are taken to procure an RMA (Return Materials Authorization) number and shipping instructions from AML.

Agency Compliance

CE

FCC Declaration of Conformity
Product Name: Model KDT750 Price Verification System
Model Number: KDT750

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This equipment may not cause harmful interference, and (2) this equipment must accept any interference received, including interference that may cause undesirable operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If you determine the equipment does cause harmful interference to radio or television reception (this may be determined by monitoring the interference while turning the equipment off and on), you are encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

2

Getting Started

This chapter gives a quick start introduction to using the KDT750.

KDT750 Startup Sequence

The KDT750 unit will begin booting the operating system once power is applied to the terminal and the rear panel is completely closed.

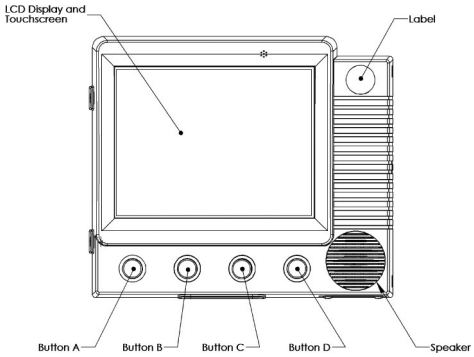
NOTE: The rear panel must be in place before the unit will power up.

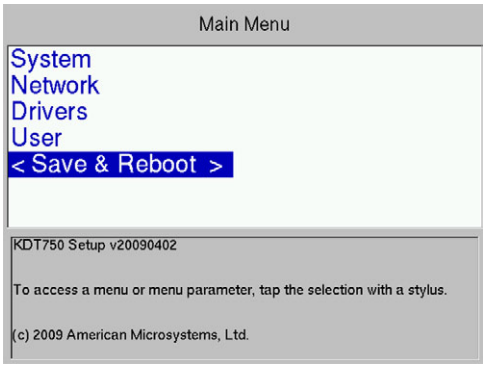
Once powered on, the KDT750 will automatically start the configured boot application.

From the factory, the unit will load default configuration settings and boot into the KDT750 home desktop.

Entering System Setup

The KDT750 System Setup can be accessed by pressing the two outer pushbuttons ("A" and "D") at the same time. After a brief delay, the unit will enter into setup mode.





NOTE: When using the KDT750 home Desktop as the boot application, the System Setup application can also be accessed through the Settings menu.

Navigating Setup

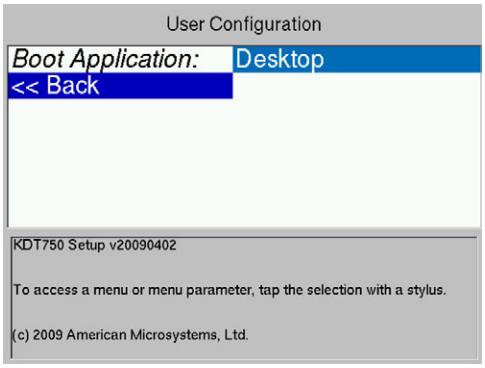
The KDT750 Setup Utility uses a simple menu interface for all system configuration options. To access a KDT750 configuration sub-menu, tap the name of the menu with a plastic stylus. To modify a configuration value, tap the option's name.

When in System Setup, the KDT750 unit will automatically reboot if there is no user activity for 5 minutes. This prevents unauthorized access into the configuration options in the event that the operator left the unit in setup mode.

Once setup is complete, the < Save & Reboot > option must be selected to write the configuration settings to the system memory.

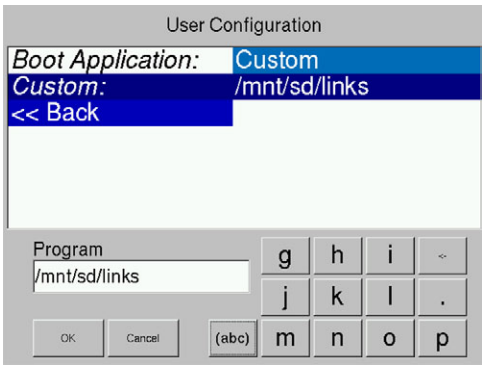
Changing the User Boot Application

To change the boot application, enter the User menu and adjust the Boot Application option to the desired program.


User Configuration
Boot Application:
Desktop
<< Back
KDT750 Setup v20090402
To access a menu or menu parameter, tap the selection with a stylus.
(c) 2009 American Microsystems, Ltd.

Selection	Description
Desktop	PC Style Desktop
APL-PCDemo	PCDemo price checking application via APL
PCT2	UniComp PCT2 emulation application
AMLVT220	VT100/220 Terminal Emulator
Links2-WWW	Web Browser
Custom	Custom command
KDT Demo	KDT750 Stand-alone Price Checking Demo

A custom application can be executed by selecting the Custom option and entering the full path to the program with the touchscreen keypad.

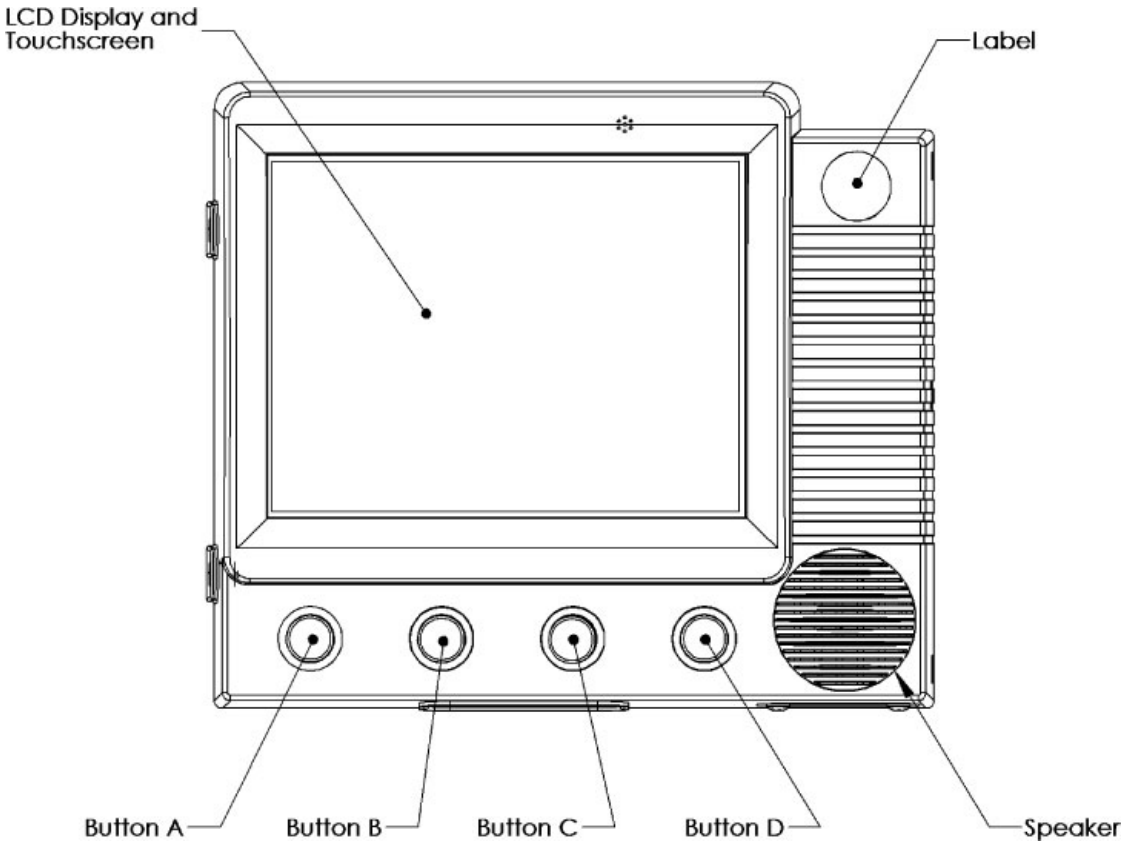


3

Terminal Overview

This chapter describes the KDT750 terminal hardware and details internal and external cable connections.

Outer Case Description



LCD Display and Touchscreen

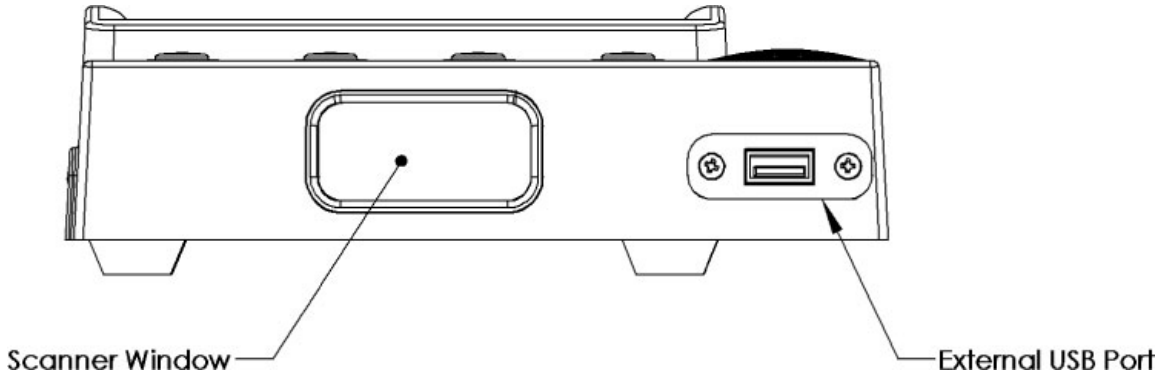
The unit features a 5.6" Full VGA (640x480 pixels) color display with an ultra-bright backlight for an unsurpassed level of viewability. The LCD is bonded to an industrial rated, resistive touch panel for user input.

Buttons A, B, C, D

The device has four programmable, momentary pushbutton type switches on the front case that can be used for special features or user input.

Speaker

A 1.5 inch, half-watt internal speaker is available for programmable tonal user feedback.

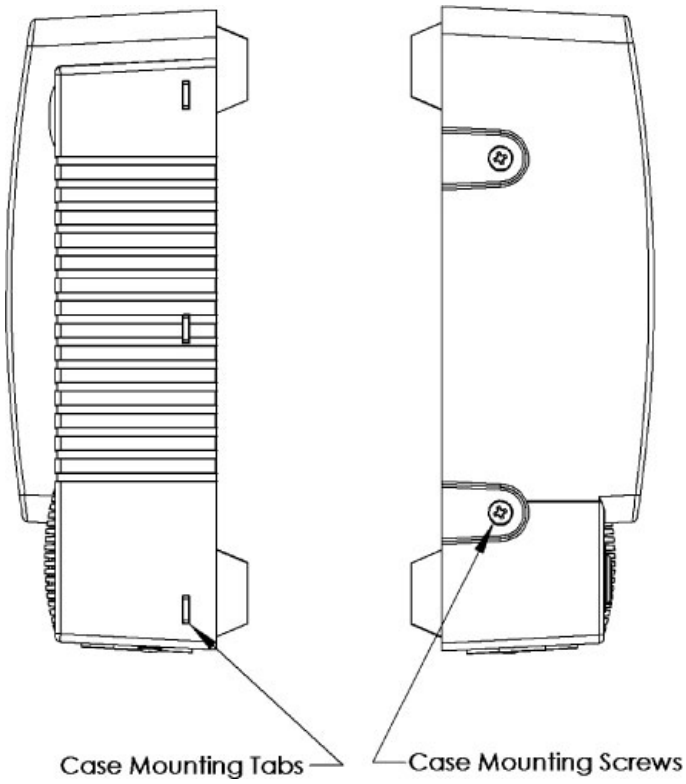


Scanner Window

The KDT750 contains an optional Linear CCD or 2-Dimensional Bar Code Decoder for decoding bar codes presented under the unit. The decoder's illumination lights will shine through the scanner window at all times. The clear protective lens should be kept clean and free of fingerprints and grime.

External USB Port

A diagnostic/administration USB port is available on the bottom of the unit to the right of the scanner window. This port can be disabled internally.



Case Mounting Tabs & Case Mounting Screws

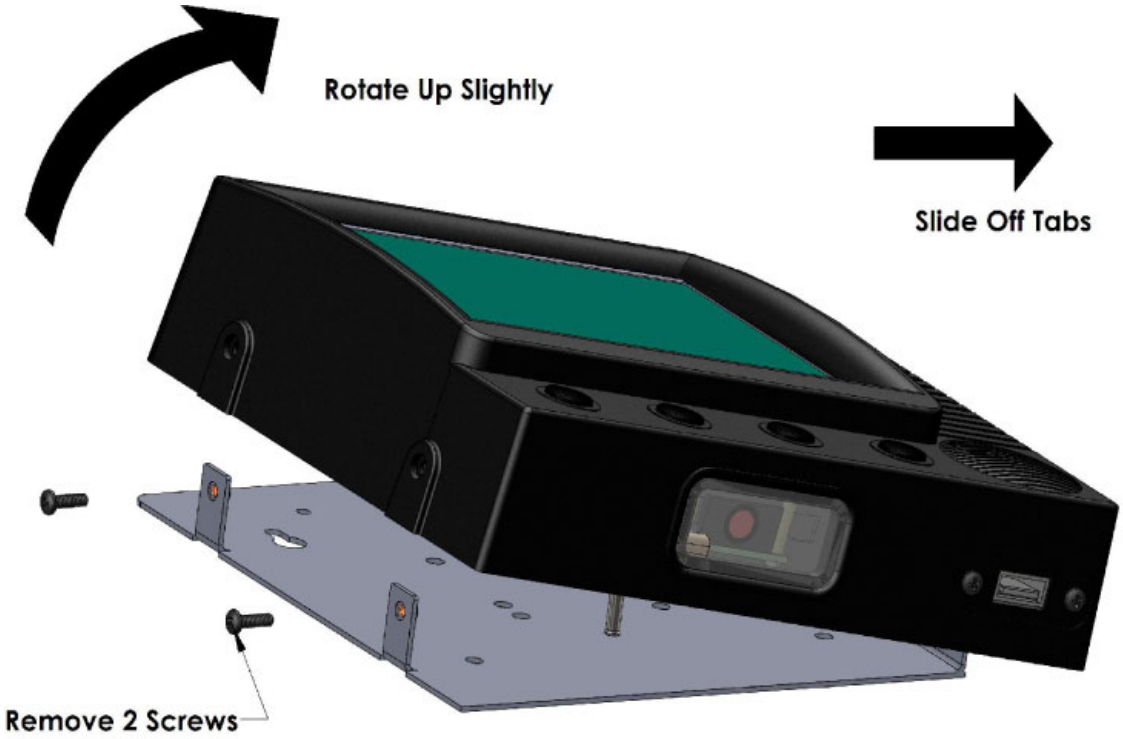
The KDT750 main outer case is held closed on the left side by two #4-40 x 1/4" screws. Longer screws should not be used, as damage to the internal components of the KDT750 can result. Then right side of the outer case contains three slots that the matching tabs of the rear panel should slide into.

Rear Panel Description

The rear panel of the unit is made from high quality 1/16" stainless steel. The panel secures the internal connections, seals the unit from dust and debris, and prevents vandalism and unauthorized access.

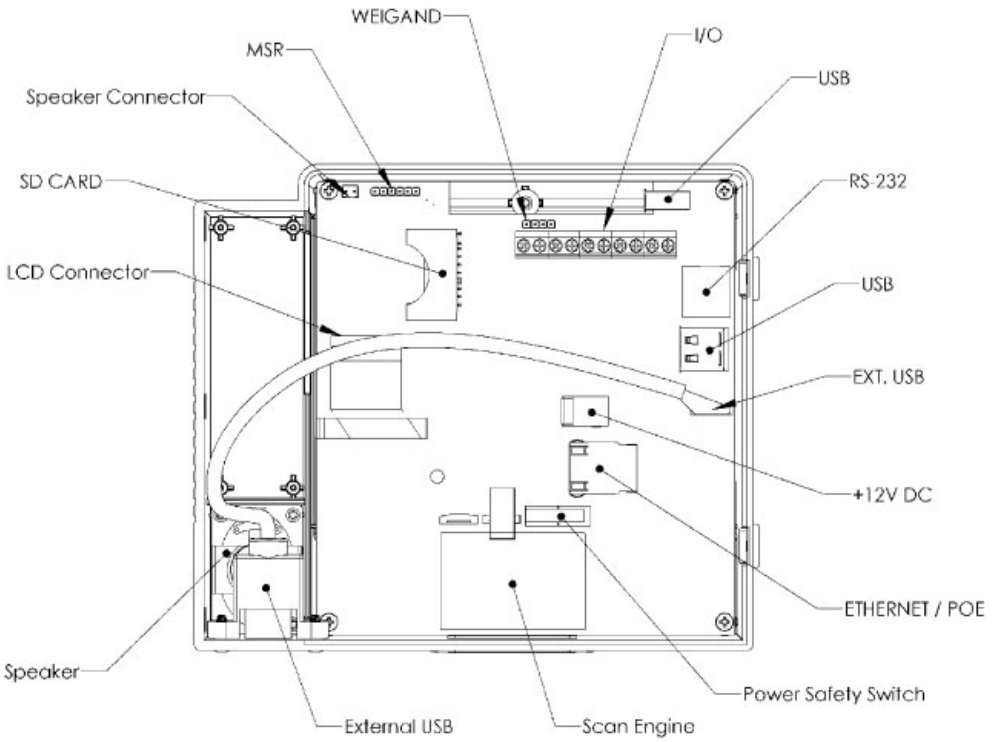
Opening the KDT750 Outer Case

In order to open the KDT750, remove the two screws on the left side and slightly rotate the outer case to the right. Once the unit is opened approximately one inch, the outer case can be slid off of the mounting tabs. All mounting brackets will remain with the rear panel, and the electronics and wiring will stay attached to the outer case.



Internal Connections

Connections to the KDT750 unit are housed internally to prevent vandalism and to secure the device.



Internal Connector Pinouts

Weigand (J3 – 4 Pin Male Header)

Pin	Description	I/O
1	Ground	
2	Data 1	I
3	Data 0	
4	+5V (Max. 0.5A)	I

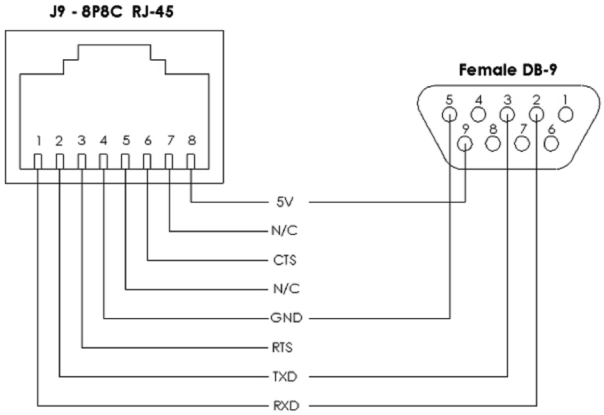
MSR (JP1 – 6 Pin Male Header)

Pin	Description	I/O
1	Ground	
2	Loop to Pin 4	I
3	RXD	I
4	Loop to Pin 2	O
5	TXD	O
6	+5V (Max. 0.5A)	

RS-232 (J9 8 - Pin RJ45)

Pin	Description	I/O
1	RXD	I
2	TXD	O
3	CTS	O
4	Ground	
5	N/C	
6	RTS	I
7	N/C	
8	+5V (Max. 0.5A)	

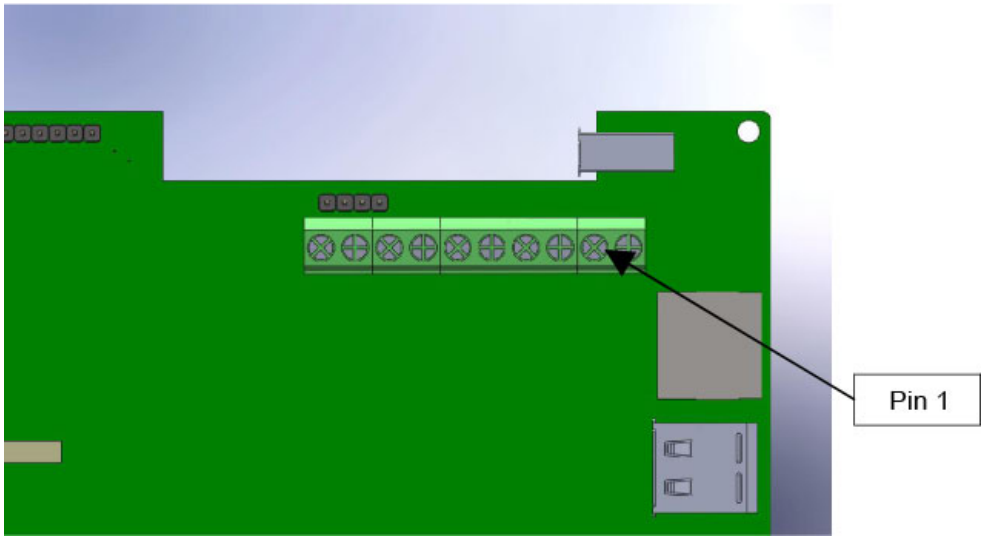
RJ-45 to DB9 Wiring Diagram



External USB Cable (JP2 - 5 Pin Male Header)

Pin	Description	I/O
1	+5V (Max. 0.5A)	
2	D-	I/O
3	D+	I/O
4	Ground	
5	Shield	

Digital I/O (J14-J17 - Screw Terminal Block)



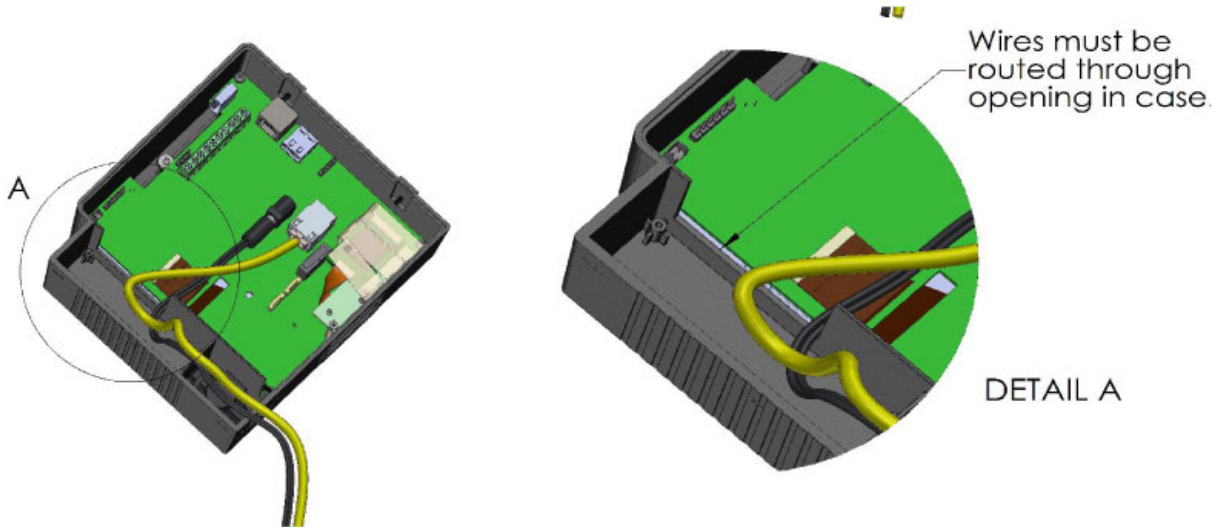
Device	Pin	Description
Relay 1	1	Contact
	2	Normally Closed
	3	Normally Open
Relay 2	4	Contact
	5	Normally Closed
	6	Normally Open
Input 1	7	High/Low
	8	Low/High
Input 2	9	High/Low
	10	Low/High

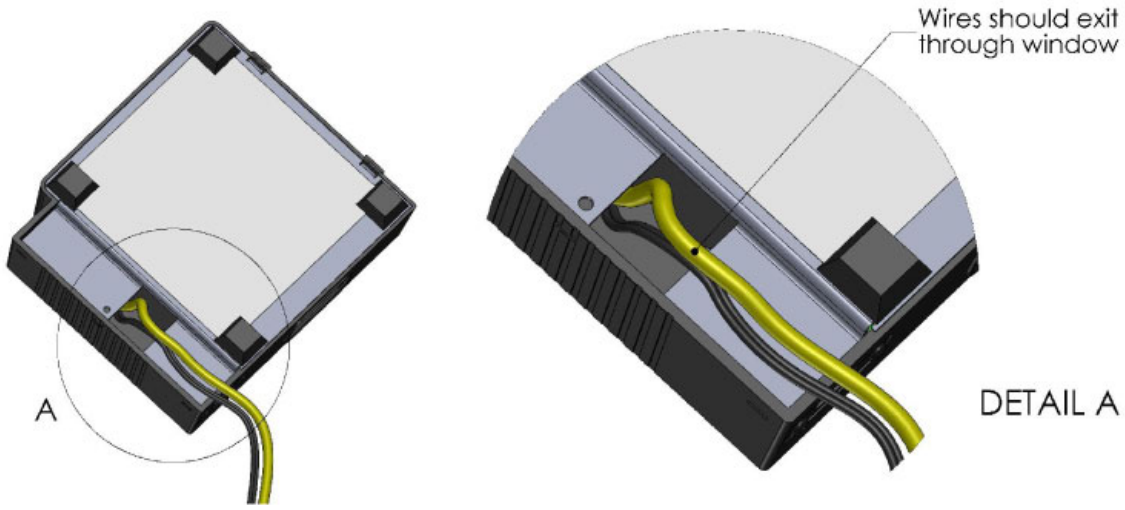
External Connections

The KDT750 houses a single external USB host port. In high security installations, this port can be disabled by disconnecting the internal cable from the port header.

Wiring Installation

To prevent vandalism and unauthorized use, all major connections to the KDT750 base unit are internally housed. All wires exiting the base unit should be routed into the recessed channel, through the opening of the divider wall in the case. The cables should then exit the rear panel through the window at the bottom of the channel.





Power Requirements and Battery Information

The KDT750 can utilize three power sources: external DC power supply, Power-over-Ethernet and an optional internal backup battery.

External DC Power Supply

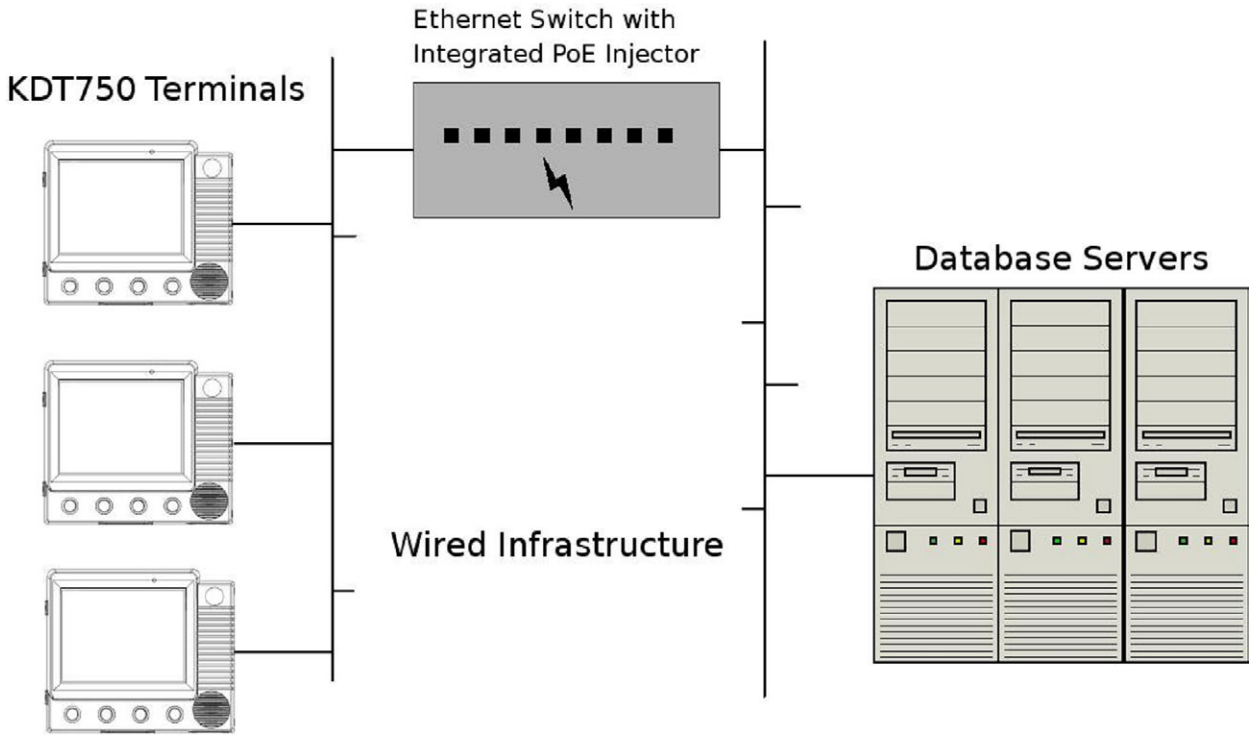
NOTE: Using power supplies that are not approved by AML for use with the KDT750 unit can cause damage to the unit and will void all warranties.

Voltage	12V, regulated
Current	1.5A
Connector	2.1mm Barrel, center positive

Internal Power-over-Ethernet Supply

The KDT750 contains a 802.3af compatible power supply. The unit can be powered via category 5 networking cable when used with an 802.3af compatible power injector. Both network data traffic and power can be sent via the same category 5 wire.

Standard	IEEE 802.3af
Class	0 (12.94 Watts)



Optional Backup Battery

If the KDT750 unit is equipped with an optional internal backup battery, the unit will continue to operate when all other power sources are lost. Depending on the configuration and usage, the backup battery should enable the unit to operate for approximately one hour.

When power is applied to the unit, the backup battery will be automatically charged. After a complete discharge, the backup battery should be charged 48 hours before use.

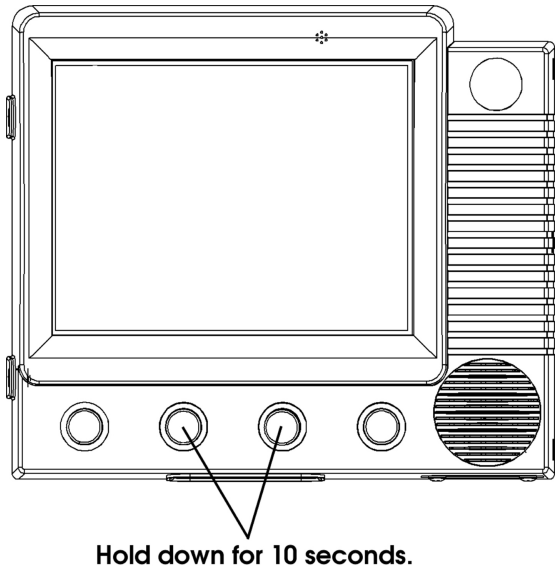
NOTE: The backup battery is permanently connected to the KDT750 motherboard. Do not attempt to remove the battery. The KDT750 unit must be properly disposed of and the battery recycled when it has reached the end of its usable life.

Type	2 Cell, Li-ion
Voltage	7.4V
Capacity	2200mAh

Main Power Switch and Power-On Reset

The KDT750 unit contains a main power switch that disables the unit when the rear panel is removed during servicing and installation. This switch is designed as a safety measure, and it is not recommended that the switch be bypassed or modified in any way.

To reset the KDT750 unit with power enabled, hold down the middle two pushbuttons for 10 seconds or until the LCD screen goes black. When the buttons are released, the unit will perform a warm boot.



Secure Digital (SD) Card

The internal SD card is required for normal operation of the KDT750 unit. The card can be removed and connected to a PC for configuration, upgrades and file transfer, but the device should not be powered on without it properly installed and secured.

All KDT750 configuration files are located on the SD card.

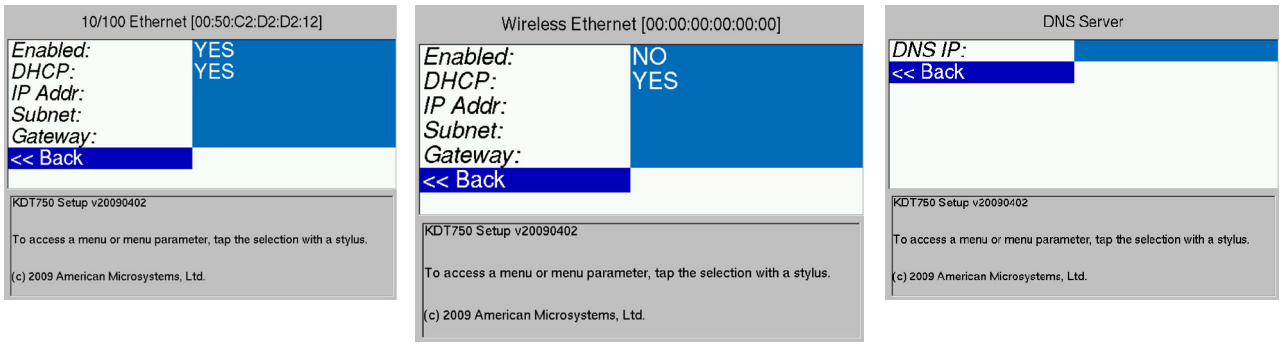
4

Communications & Input

This chapter describes the communication capabilities of the KDT750.

Network Communications

The KDT750 relies on either the built-in 10/100 BaseTX Fast Ethernet network adapter or the optional 802.11b/g/n wireless radio for communicating with a host server. General network settings and device selection is made through the *network.settings* file or the KDT750 Setup Utility.



NOTE: All wireless SECURITY settings are configured in the wifi.conf file described in Chapter 5.

Option	network.settings Parameter	Description	Valid Values	Use	Example
Wired Ethernet Enable	eth_enable	Enable 10/100 BaseTX Ethernet Port	1 0	Enable Disable	eth_enable=1
Wired DHCP	eth_dhcp	Set DHCP for Ethernet Port	1 0	Enable Disable	eth_dhcp=1
Wired Static IP	eth_ip	Ethernet Static IP Address when eth_dhcp is set to 0			eth_ip=192.168.100.101
Wired Static Subnet Mask	eth_subnet	Ethernet Subnetwork Mask			eth_subnet=255.255.255.0
Wired Static Gateway	eth_gateway	Ethernet default routing gateway			eth_gateway=192.168.100.1
Wireless Radio Enable	wifi_enable	Enable 802.11 radio	1 0	Enable Disable	wifi_enable=1
Wireless DHCP	wifi_dhcp	Set DHCP for radio	1 0	Enable Disable	wifi_dhcp=1
Wireless Static IP	wifi_ip	Radio static IP Address when wifi_dhcp is set to 0			wifi_ip=192.168.100.1
Wireless Subnet Mask	wifi_subnet	Radio Subnetwork Mask			wifi_subnet=255.255.255.0
Wireless Gateway	wifi_gateway	Radio default routing gateway			wifi_gateway=192.168.100.2
Static Domain Name Server	dns	DNS Server to use			dns=192.168.100.2

Example network.settings (Only using Ethernet with DHCP)

```
eth_enable=1
eth_dhcp=1
wifi_enable=0
```

Example network.settings (Only using Ethernet with Static Addressing)

```
eth_enable=1
eth_dhcp=0
eth_ip=192.168.100.101
eth_subnet=255.255.255.0
eth_gateway=192.168.100.1
wifi_enable=0
dns=192.168.100.2
```

Example network.settings (Only using 802.11 Radio with DHCP)

```
eth_enable=0
wifi_enable=1
wifi_dhcp=1
```

Serial Communications

The KDT750 contains two user accessible RS-232 ports and one bar code scanner port for serial communications with a PC or other peripheral devices. Each port is capable of baud rates up to 115.2 Kbps.

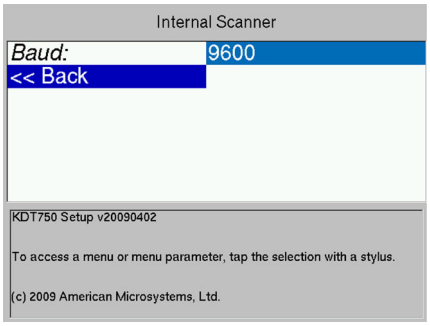
Serial communication ports are used to communicate with devices such as:

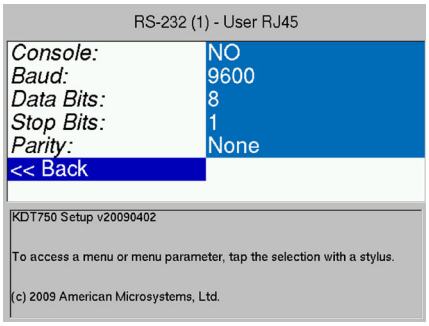
- Internal Bar Code Scanner
- External Bar Code Scanner
- External Magnetic Stripe Reader
- Serial Printer
- PC

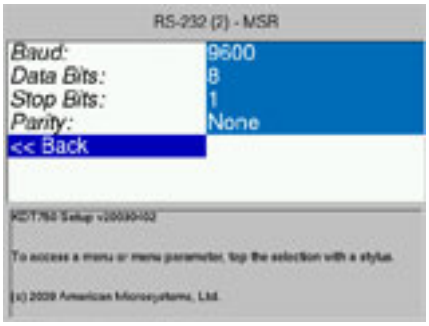
The serial.settings file is used to configure the three RS-232 serial ports on the KDT750. Each port is designed for a specific function and may or may not be used deepening on the KDT750's hardware configuration:

Port Number	Normal Function	Linux Device Name	Connector
0	Internal Bar Code Decoder	/dev/ttySAC0	J19 & J20 (12 Pin FPC Flex Connectors)
1	Debug Console and User RS-232	/dev/ttySAC1	J9 (8 Pin RJ-45 Type Jack)
2	Magnetic Stripe Reader	/dev/ttySAC2	JP1 (6 Pin Male Header)

The serial ports can be configured from the Driver menu of setup. The ports will be configured with these settings on boot.







Option	serial.settings Parameter	Description	Valid Values	Use	Example
Internal Scanner Baud Rate	port0baud	Baud rate for internal bar code scanner	9600	Internal Scanner	port0baud=9600
Port 1 Baud Rate	port1baud	Baud rate for RJ-45 RS-232	9600 19200 38400 57600 115200		port1baud=115200
Console on Port 1	port1console	Enable debug console on RS-232 port	1 0	Enabled Disabled	port1console=1
Data Bits	port1bits	Set number of data bits for port 1	7 8		port1bits=8
Parity	port1parity	Parity setting for port 1	N E O	No Parity Even Parity Odd Parity	port1parity=N
Stop Bits	port1stop	Set number of stop bits for port 1	1 2		port1stop=1
Port 2 Baud Rate	port2baud	Baud rate for MSR	9600 19200 38400 57600 115200		port2baud=9600
Data Bits	port2bits	Set number of data bits for port 2	7 8		port2bits=8
Parity	port2parity	Parity setting for port 2	N E O		port2parity=N port2stop=1
Stop Bits	port2stop	Set number of stop bits for port 2	1 2		

Example serial.settings (Linear CCD Scan Engine, Debug Console on Port 1)

```
port0baud=9600
port1baud=115200
port1console=1
port1bits=8
port1parity=N
port1stop=1
port2baud=9600
port2bits=8
port2parity=N
port2stop=1
```

Example serial.settings (2D Omni-directional Imager Scan Engine)

```
port0baud=9600
port1baud=115200
port1console=0
port1bits=8
port1parity=N
port1stop=1
port2baud=9600
port2bits=8
port2parity=N
port2stop=1
```

USB Communications

The unit contains three user accessible USB 1.1 Full speed host ports, capable of data rates up to 12 Mbps.

Common USB devices that can be used with the KDT750 are:

- External Bar Code Scanner
- External Magnetic Stripe Reader
- External Keyboard
- USB storage devices ("thumb" or "pen" drives)

No configuration is necessary for USB devices that are compatible with the KDT750.

Digital I/O

The KDT750 base unit contains two electrically isolated digital inputs and two electrically isolated digital outputs.

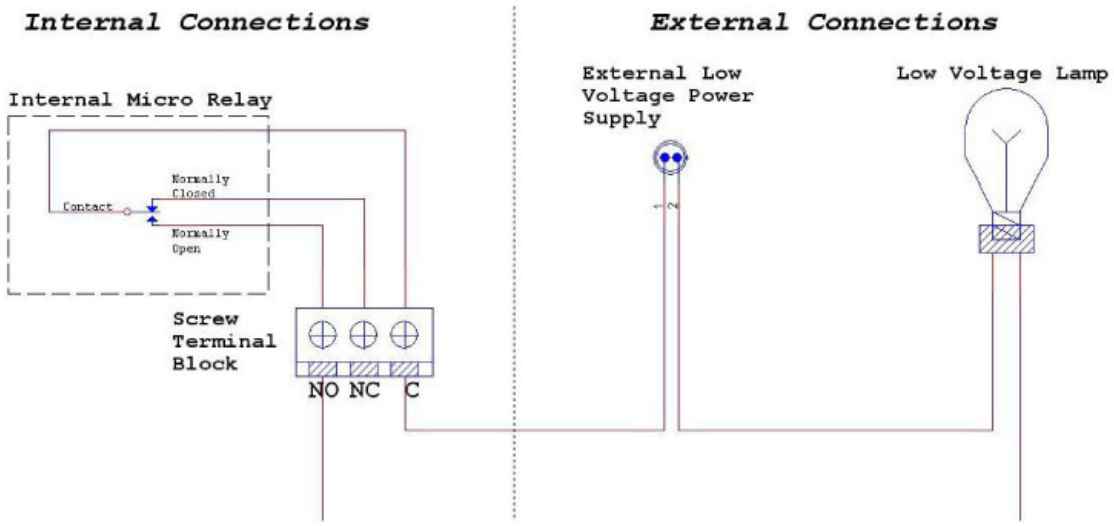
Digital Outputs (Micro-Relays)

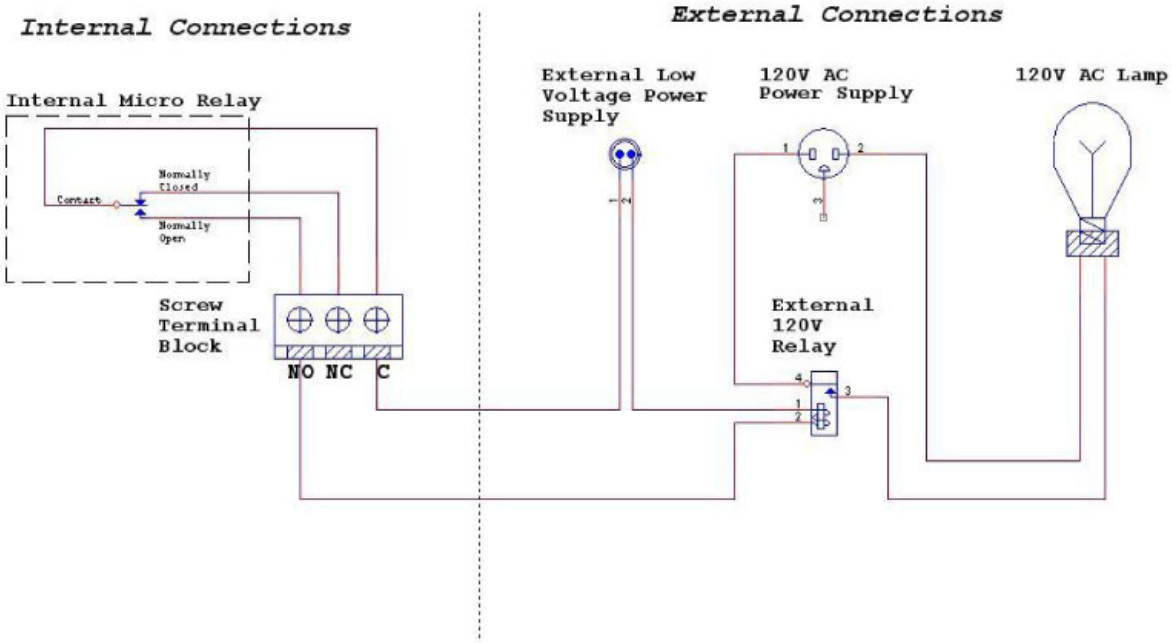
The KDT750 digital outputs are controlled via internal micro-relays driven by the microprocessor. These relays can be used to drive external devices such as:

- Lights and Beacons
- Door Strikers
- Sirens
- Stationary Scanners

The internal relays are designed for low voltage applications. To use the relays in high voltage situations, an additional external rely should be implemented.

Relay Wiring Diagrams



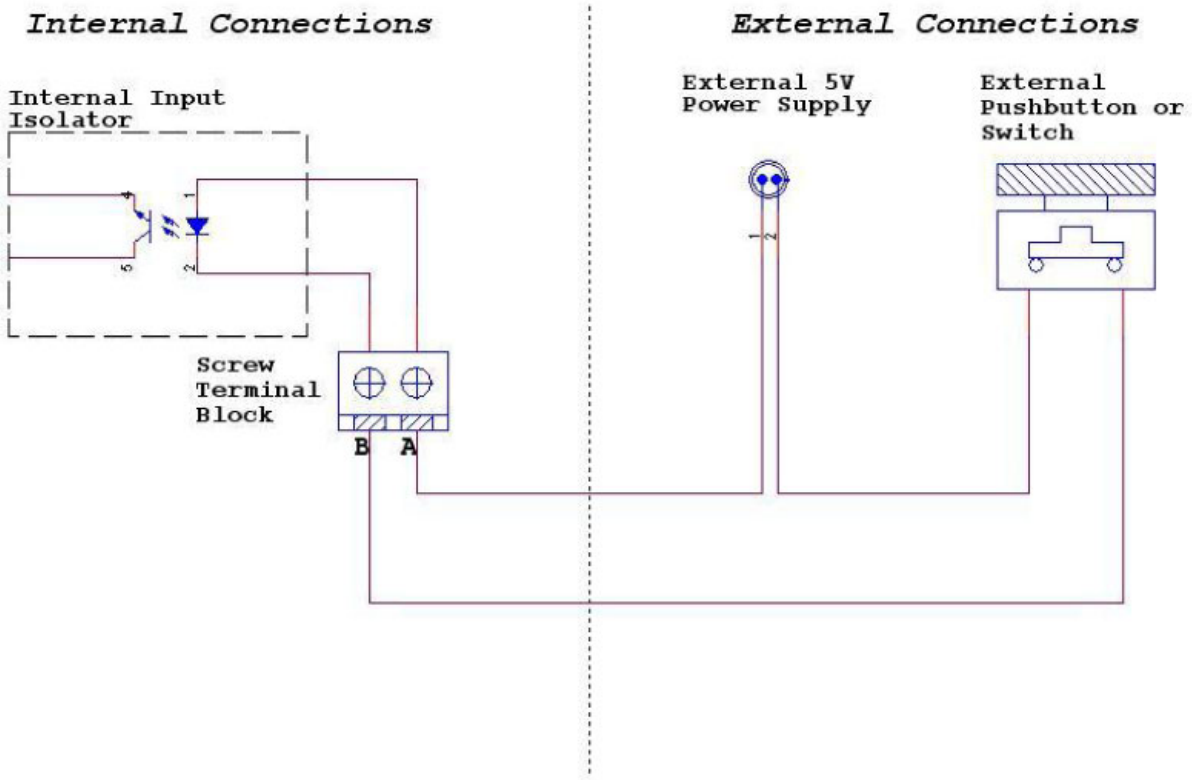


Digital Inputs (Opto-Isolators)

The KDT750's internal digital inputs can be used to signal events and actions from an external source. Possible uses for the isolated input are:

- External Pushbutton Switches
- Door Sensors
- Proximity Sensors

Digital Input Wiring Diagram

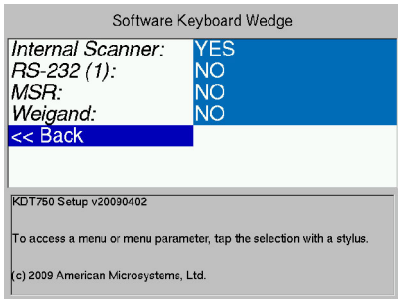


Weigand Interface

The Weigand interface is used to connect proximity card and smart card readers to the KDT750. Weigand is a simple, two-wire interface used to transmit unidirectional data from a peripheral device to a host.

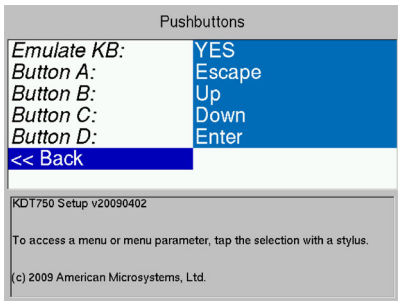
Software Keyboard Wedge

A software keyboard wedge can be used to convert data coming from one or more external hardware devices into a usable keyboard input.



Pushbutton Input

The KDT750 panel pushbuttons can emulate PC keyboard key presses.



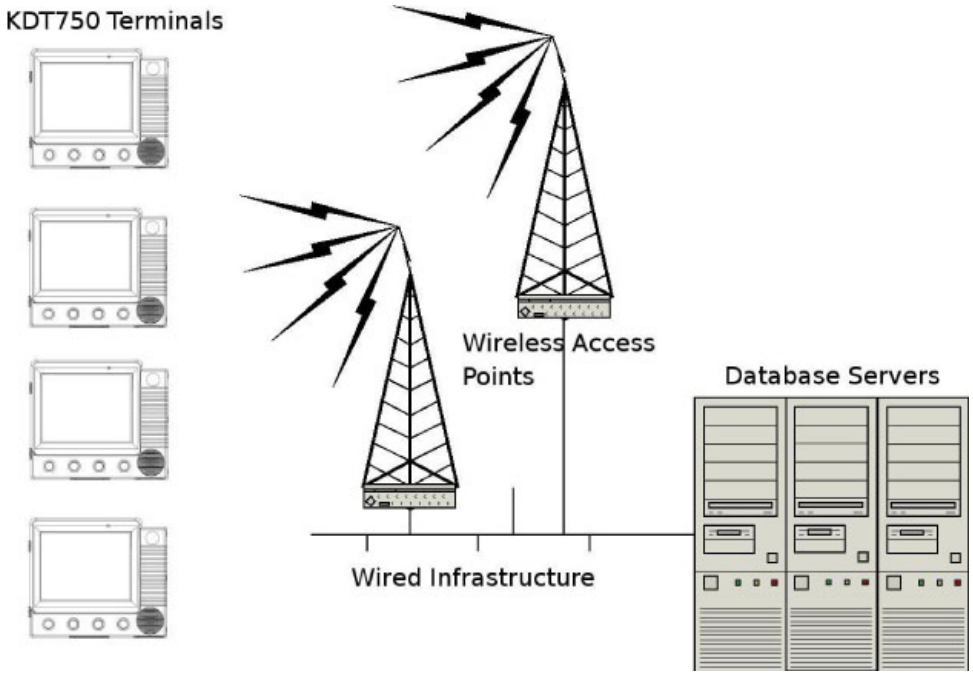
5

Wireless Networking

This chapter describes the configuration of the optional internal 802.11 radio.

Overview

The KDT750 terminal can contain an optional 802.11b/g/n radio and internal antenna. This radio is specifically designed to communicate with any 802.11b/g or 802.11n (Draft v2.0) Access Point.



The range of the radio depends greatly on the quality of the Access Point and the RF communications characteristic of the environment where the device is used. The typical range for an 802.11 radio is 500 feet through free air. Additional Access Points must be added to improve coverage in a larger area, or in electrically noisy RF environments.

802.11 Fallback

Wireless LAN technology is designed to make maintaining a connection between two devices as reliable and consistent as possible. Since the speed of the connection between wireless devices will vary as range and signal quality varies, the wireless devices will intentionally sacrifice throughput (data rate or connection speed as measured in bits per second) in exchange for maintaining a reliable connection. In other words, a reliable connection at a lower speed is preferred over an unreliable connection at a higher speed (i.e., it is easier to maintain the connection if data rate is deliberately reduced, or put another way, lower data rates will tolerate a higher range and/or worse signal quality). This characteristic is known as fallback. As example, an 802.11b system will fallback from 11 Mbps to 5.5 Mbps as range increases or signal quality decreases. Subsequent fallbacks from 5.5 Mbps to 2 Mbps and 1 Mbps are also supported.

Interference and Coexistence

802.11 operates in a range of radio frequencies known as an "unlicensed" band (i.e., the FCC does NOT require the use of a license in order to operate a radio transmitter in this range). This means that commercially available radio devices other than wireless LAN devices are permitted to use the same frequency band as 802.11. Consequently, these co-existing radio devices can interfere or "jam" the wireless LAN (and vice versa). The most troublesome devices are cordless telephones and microwave ovens.

Fortunately, higher quality cordless phones tend to "listen" for a clear channel before becoming active and will thus avoid interfering with a wireless LAN (i.e., the cordless phone seeks a clear channel for itself so naturally avoids being interfered with or being a source of interference). Jamming from microwave ovens is more severe but is usually restricted to the upper frequency range for 802.11 (it should be noted that 802.11b/g divides the available frequency band into 11 channels (US). The higher numbered channels are most susceptible to microwave oven interference).

In each instance, jamming occurs only when the cordless telephone or microwave oven is active.

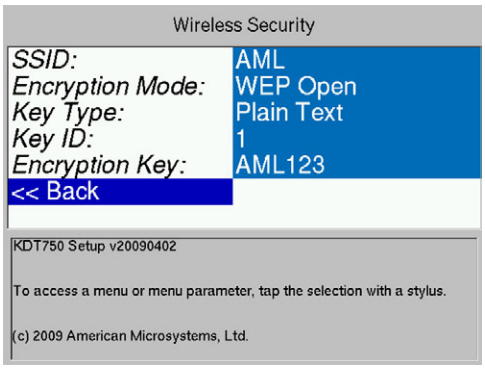
Encryption and Authorization

Much has been publicized in the mass media recently about security problems with wireless LANs. Although it cannot be denied that some encryption algorithms currently used in 802.11 are flawed, the fact is that security breaches of a wireless LAN require a deliberate attempt to access the network by an intruder.

The primary issue is that many current users of wireless LAN have opted NOT to turn on security features. If users were to enable the security features currently available (including only allowing known systems access to the network and enabling WEP (Wired Equivalent Privacy) or WPA (Wifi Protected Access)) on even the most basic access points, the intruder's work is much harder. Much as a burglar will stray away from a house whose doors and windows are securely locked, so too will an attacker tend to move past a wireless network when even the simplest security measures are enabled.

Wireless Configuration

The optional 802.11b/g/n radio can be configured with the KDT750 Setup Utility under the Network menu.



Some advanced features are not configurable with the utility and manual configuration of the settings may be necessary by editing the wifi.conf configuration file. This file is a standard ASCII encoded text file that is readable and writable by any text editor. Empty lines and lines starting with a # character will be ignored. The file begins with two mandatory definition parameters that MUST be included in all wireless configuration files for the KDT750:

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
```

This tells the wireless security supplicant how to set up the radio interface. The file then includes a network block header that will be followed by all wireless network parameters and security settings that should be used by the connection. A close brace '}' will follow the parameters:

```
network={

<<<List of 802.11 configuration parameters>>>

}
```

Multiple valid network blocks can be defined in the configuration file. The unit will try all valid network blocks until the device is associated with an AP.

NOTE: Care should be taken when defining multiple network blocks because in some configurations it is possible to associate with an AP but not be able to transmit or receive data. In these cases, the unit will not know to move on to the next network block because the radio sees a valid association with the AP.

Wireless Configuration Parameters

Inside a network block of the configuration file will be all the necessary parameters to configure the interface.

Parameter	Description	Valid Values	Use	Example
ssid	Wireless Network Name (ESSID)			ssid="MyNetwork"
key_mgmt	Encryption key management method to use	NONE	No Dynamic Encryption (No Encryp-tion or WEP Encrpytion)	key_mgmt=WPAPSK
		WPA-PSK	Use WPA/WPA2 Pre-shared Key	
		WPA-EAP	Use WPA/WPA2 Authentica-tion and keying	
		IEEE8021X	Use 802.1x supplicant authentica-tion (Used for LEAP)	
scan_ssid	Scan for hidden Networks (APs not broadcasting)	1	Enable hidden scan	scan_ssid=1
		0	Only allow networks that are broadcasting SSIDs	
auth_alg	WEP Authentication method	OPEN	Use open WEP system	auth_alg=OPEN
		SHARED	Use shared key WEP system	
wep_tx_keyidx	WEP transmission key to use for encryption of outgoing data	0	Use first key (0)	wep_tx_keyidx=0
		1	Use second key (1)	
		2	Use third key (2)	

Parameter	Description	Valid Values	Use	Example
		3	Use fourth key (3)	
wep_key0 wep_key1 wep_key2 wep_key3	WEP Encryption keys	ASCII text encoded keys should be encompassed in '"'s and hex encoded keys should not		wep_key0=0a0b0c0d0e wep_key1="MYTEXTWEPKEY1" wep_key2=1122334455 wep_key3="MYOTHERWEPKEY"
psk	WPA/WPA2 Pre-shared key	ASCII text encoded keys should be encompassed in '"'s and hex encoded keys should not		psk="123456789"
eap	WPA/WAP2 EAP algorithm	PEAP	Use PEAP	eap=PEAP
		TLS	Use TLS	
		TTLS	Use TTLS	
phase1	Outer EAP authentication	"peaplabel=0"	Existing PEAP label	phase1="peaplabel=0"
		"peaplabel=1"	Force new PEAP label	
phase2	Inner EAP authentication	"auth=MSCHAPV2"	EAP-PEAP	phase2="auth=MSCHAPV2"
		"autheap=MSCHAPV2 autheap=MD5"	EAP-TTLS	
identity	WPA/WPA2 Username			identity="MyUsername"
password	WPA/WPA2 Password or Passphrase			password="MyPassword"
ca_cert	Local client certificate file			ca_cert="/mnt/sd/ca.pem"
private_key	Local private encryption key file			private_key="/mnt/sd/client.p12"
private_key_passwd	Password to decode local private encryption key file			private_key_passwd="MyKeyPassword"

Example Configurations

The following are example text that could be entered into the wifi.conf file. These examples in the plain file format are available on the KDT750 product CD.

Plain text connection (No Encryption, No Authorization, AP Broadcasting SSID)

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=NONE
}
```

Plain text connection with hidden SSID

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=NONE
scan_ssid=1
}
```

Open WEP Encrypted with hidden SSID, WEP Keys in Text Format

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=NONE
scan_ssid=1
auth_alg=OPEN
wep_tx_keyidx=0
wep_key0="MYTEXTWEPKEY0"
wep_key1="MYTEXTWEPKEY1"
wep_key2="MYTEXTWEPKEY2"
wep_key3="MYTEXTWEPKEY3"
}
```

Exact Configuration as Above but with WEP Keys in Hex Format

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=NONE
```

```
scan_ssid=1
auth_alg=OPEN
wep_tx_keyidx=0
wep_key0=4D595445585457455048455930
wep_key1=4D595445585457455048455931
wep_key2=4D595445585457455048455932
wep_key3=4D595445585457455048455933
}
```

WPA/WPA2 with Pre-Shared Key (PSK)

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=WPAPSK
psk=”123456789”
}
```

Exact Configuration as Above but with raw Pre-Shared Key (PSK)

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=WPAPSK
psk=469100a17577fd350ac9e09acd2399b56145e76a22b8183ff311f1c207c93d3a
}
```

WPA/WPA2 Enterprise with EAP-PEAP/MSCHAPv2)

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=WPAEAP
eap=PEAP
phase1="peaplabel=0"
phase2="auth=MSCHAPV2"
identity="MyUsername"
password="MyPassword"
}
```

WPA/WPA2 Enterprise with EAP-TLS and local certificates

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
```

```
ssid="MySSID"
key_mgmt=WPAEAP
eap=TLS
identity="MyUsername"
ca_cert="/mnt/sd/ca.pem"
private_key="/mnt/sd/client.p12"
private_key_passwd="MyKeyPassword"
}
```

WPA/WPA2 Enterprise with EAP-TTLS (Tunneled TLS), no local certificates

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=WPAEAP
eap=TTLS
phase1="peaplabel=0"
phase2="auth=MSCHAPV2"
identity="MyUsername"
password="MyPassword"
}
```

Cisco Lightweight EAP (LEAP) with dynamic WEP keys

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
ssid="MySSID"
key_mgmt=IEEE8021X
eap=LEAP
identity="MyUsername"
password="MyPassword"
}
```

6

Integrated Bar Code Scanner

This chapter describes the use of the internal bar code reader.

Overview

The KDT750 terminals can contain an integrated bar code reader for decoding bar code symbols in a variety of formats.

The terminal can be equipped with a linear CCD bar code decoder, a 2-Dimensional, Omni-directional decoder or no bar code scan engine at all.

It is important to know what type of engine is installed in the unit to allow for correct customization of the engine.

Determining Scanner Type

The type of the internal scanner can be determined either by the KDT750's model number reference chart at the beginning of this document or by observing the scanner's decode pattern.

If the KDT750 model number ends in a zero, the unit contains no internal scan engine:
KDT750-xxx0

If the KDT750 model number ends in a one, the unit contains the Linear CCD laser:
KDT750-xxx1

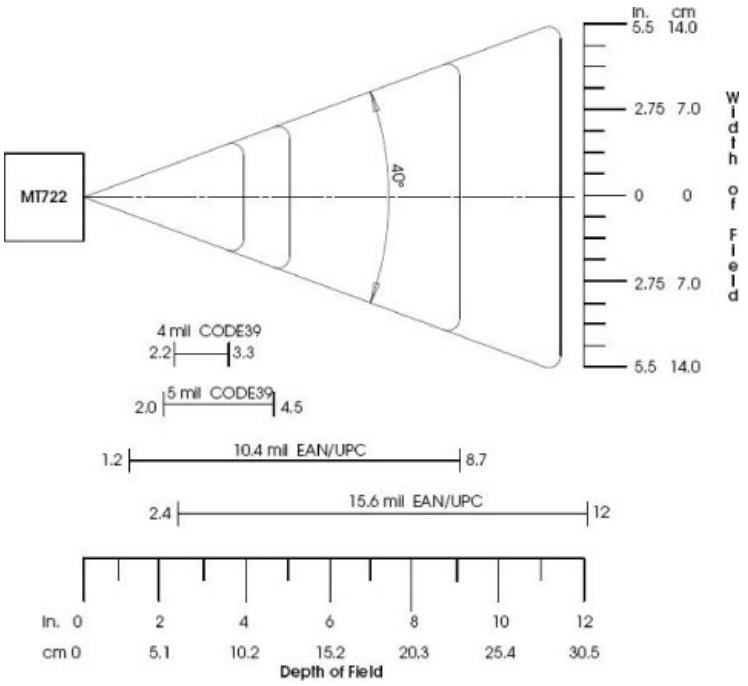
If the KDT750 model number ends in a two, the unit contains the 2D Omni-directional imager:
KDT750-xxx2

If the KDT750 model number ends in a three, the unit contains the 1D Laser engine:
KDT750-xxx3

If the KDT750 model number ends in a four, the unit contains the External Omni-directional engine:
KDT750-xxx4

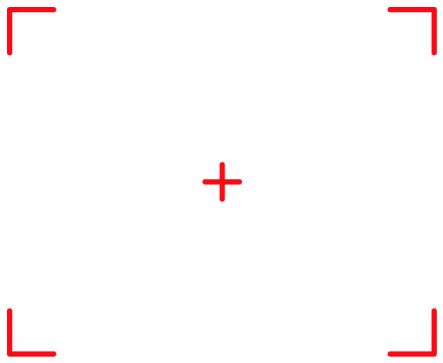
Linear CCD Decode Zones

The Linear CCD can only read symbols that are within its field of view:



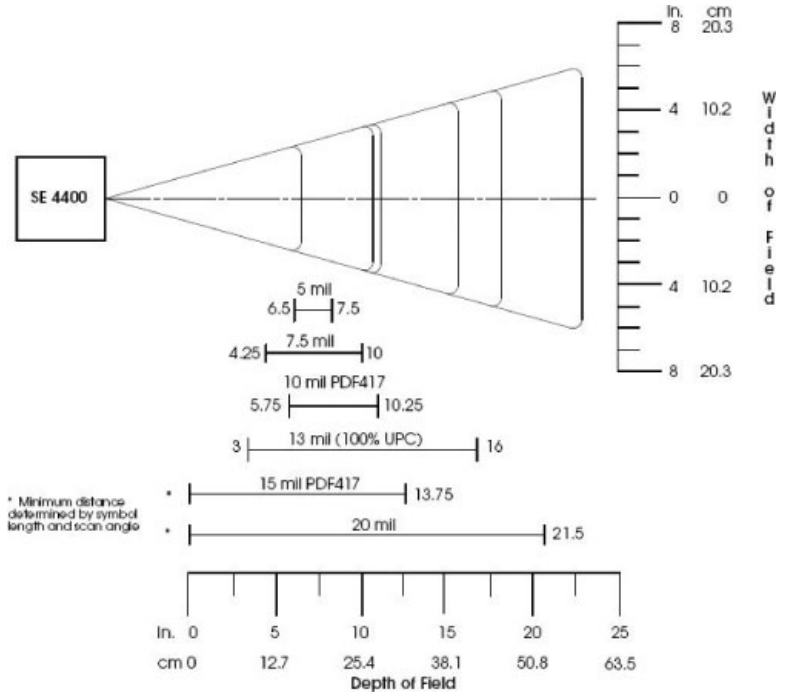
2D Omni Scanner Aiming System and Decode Zones

The 2D Omni-directional scanner will use a 650nm laser to draw an aiming pattern of the decoder's decode zone:

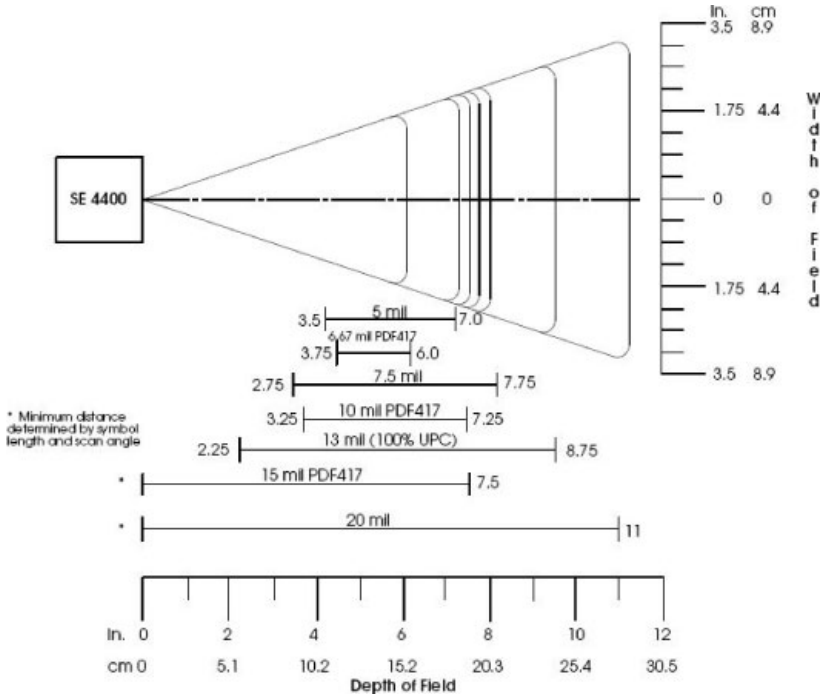


The decoder is only capable of decoding symbols that are within its field of view. Two focus modes are selectable for the 2D imager:

Far Focus:



Near Focus:


In. cm
3.5 8.9
1.75 4.4
0 0
1.75 4.4
3.5 8.9
Width of Field
SE 4400
3.5 5 mil 7.0
3.75 6.67 mil PDF417 6.0
2.75 7.5 mil 7.75
3.25 10 mil PDF417 7.25
2.25 13 mil (100% UPC) 8.75
* 15 mil PDF417 7.5
* 20 mil 11
* Minimum distance determined by symbol length and scan angle
In. 0 2 4 6 8 10 12
cm 0 5.1 10.2 15.2 20.3 25.4 30.5
Depth of Field

Triggering

The KDT750's internal bar code scanners are designed to be used in presentation modes. In these modes, the scanner is always scanning and looking for bar codes to decode.

NOTE: Some internal scanners have the ability to disable the illumination LEDs when no bar code is present under the scanner. The scanner is still looking for bar codes, but is saving power by only enabling the illumination when a new bar code symbol is present.

To manually trigger the bar code decoder, use the *Data Viewe*r tool under the *System Tools* folder.

Scanning Bar Codes

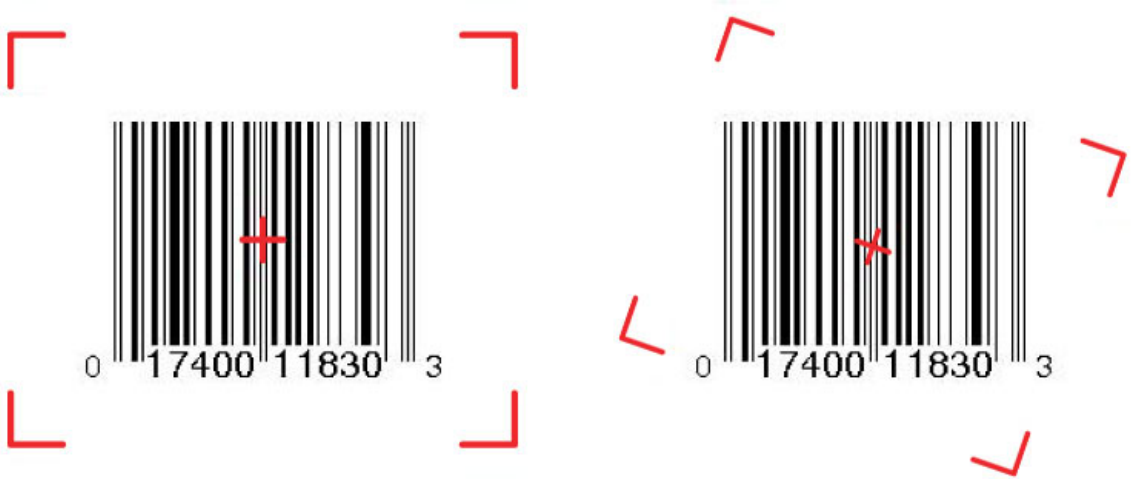
NOTE: Bar codes will only be scanned when software that is aware of the bar code interface is running (PCDemo, KDT750 Demo, Data Viewer, etc...)

Scanning with the Linear CCD

KDT750 units equipped with the Linear CCD scan engine require proper alignment of the bar code under the scanner window. The Linear CCD's ideal scanning range is between 2.5 inches and 8 inches.

Scanning with the Omni-Directional Imager

The 2D Omni-directional imager is capable of scanning bar codes at any orientation as long as the entire symbol is visible to the scanner and illuminated.



Supported Symbologies

Symbology	Linear CCD	2D Imager
UPC/EAN	X	X
Code 39	X	X
Code 93	X	X
Code 128	X	X
Interleaved 2 of 5	X	X
Discrete 2 of 5	X	X
MSI/Plessy	X	X
Codabar	X	X
Code 11	X	X
GS1 (Formerly RSS)	X	X
Postal Codes	(Chinese Only)	X
Composite Codes		X
PDF417		X
MicroPDF417		X
Maxicode		X
Data Matrix		X
QR Code		X

Obtaining and Using Setup Bar Codes

The internal bar code scanners can be configured with special setup bar code symbols. These symbols are specific to the model of bar code scanner installed in the unit and are available from AML.

The default parameters and trigger mode bar codes are listed below.

NOTE: The unit will NOT make an audible beep after scanning a setup bar code.

Parameter	Linear CCD	2D Omni-directional Imager
Set All Defaults	Parameters Default	Parameters Default
Set Decode Mode	Continuous Decoding (Always On)	Continuous Decoding (Always On)
Set Focus	N/A	Focus Near Focus Far Smart Focus (Alternate between near and far)

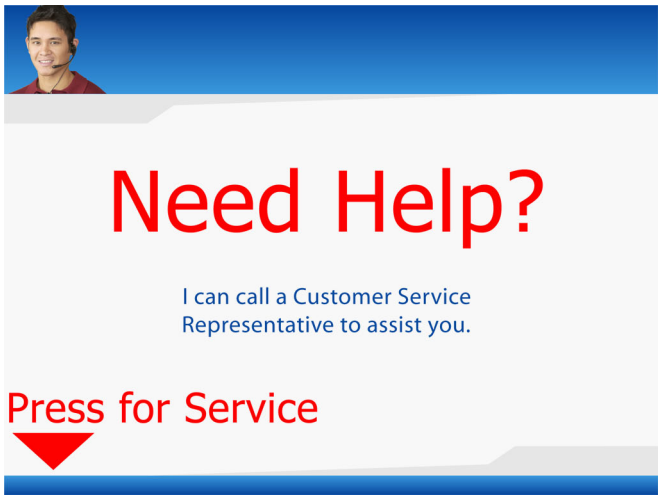
7

Installed Software

This chapter describes the preinstalled software suite on the KDT750.

PCDemo

PCDemo is a versatile client application designed to run natively on the AML KDT750 price checking unit. PCDemo handles data capture and processing, network communication with a database server, and all user interface and display attributes for data lookup and verification applications.



More information on PCDemo can be found by viewing the KDT750 APL Guide. See the Related Documents section in Chapter 1 for more information.

KDT750 Demo

The KDT750 Demo application is a standalone demo of the capabilities of the KDT750. It is based on the PCDemo software, but requires no network or external database. Internally, it includes a small number of bar codes that can be scanned to simulate a database lookup.

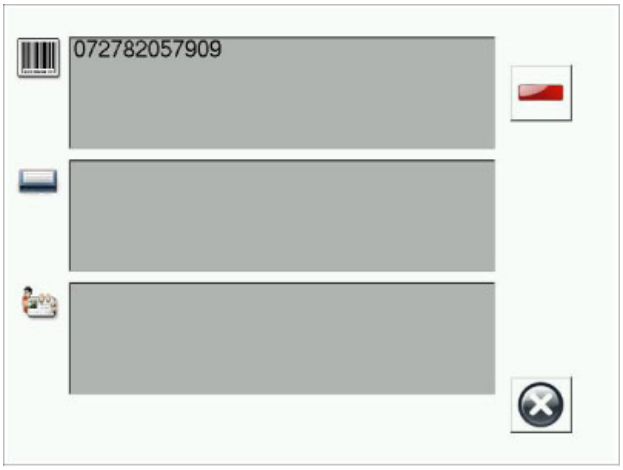
Part Number	Description	Price
070074577128	Similac Go & Grow\n Soybased Formula\n 24 oz.	19.95
051500240908	Jif Creamy Peanut Butter\n 40 oz.	3.60
027000486061	Orville Redenbachers\n Gourmet Popping Corn	2.95
021000658831	Kraft\n Macaroni & Cheese Dinner\n 7.25 oz.	0.79
024000162896	Del Monte\n French Style Green Beans\n 14.5 oz.	0.89
051500253625	Crisco Pure\n Vegetable Oil\n 48 fl. oz.	4.79
017400118303	Minute Rice\n 14 oz.	2.69
070870001001	Mrs. Baird's Extra Thin\n Sliced White Bread	2.79
038000029707	Kellogg's Apple Jacks\n 19.1 oz.	2.29
024000013709	Del Monte\n Tomato Sauce\n 8 oz.	8.89

Bar Code Data Viewer

The KDT750 contains a simple application called *Data Viewer* that demonstrates and verifies the configuration of various input devices. *Data Viewer* is located in the *System Tools* folder.

Data Viewer displays a field for each of the standard input devices:

- Internal Bar Code Reader
- External Magnetic Stripe Reader
- External Proximity Card Reader



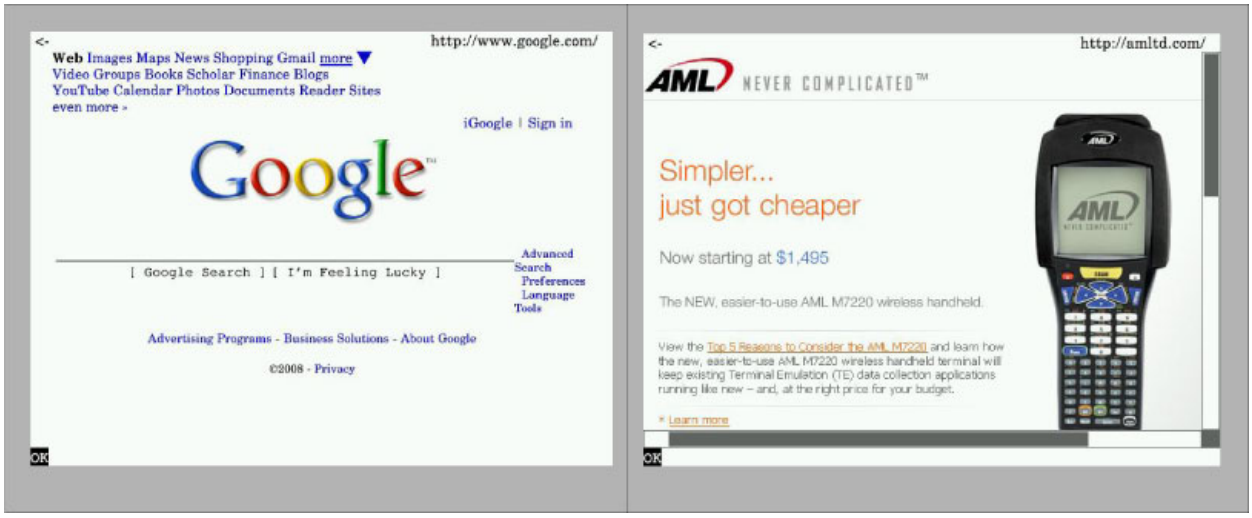
Web Browser

The KDT750 includes Links2, a built-in HTTP web browser for fetching and displaying web pages. The application's icon is located under the Network folder.

Links2 capabilities include:

- HTML 4.0 support (without CSS)
- HTTP 1.1 support
- HTTPS (SSL) support
- Text or graphical mode
- Tables and frames in both modes
- Bookmarks
- Background file downloads

Graphics Mode


<-
http://www.google.com/
Web Images Maps News Shopping Gmail more
Video Groups Books Scholar Finance Blogs
YouTube Calendar Photos Documents Reader Sites
even more »
iGoogle | Sign in
Google
[Google Search] [I'm Feeling Lucky]
Advanced Search
Preferences
Language Tools
Advertising Programs - Business Solutions - About Google
©2008 - Privacy
OK
<-
http://amltd.com/
AML NEVER COMPLICATED™
Simpler...
just got cheaper
Now starting at $1,495
The NEW, easier-to-use AML M7220 wireless handheld.
View the Top 5 Reasons to Consider the AML M7220 and learn how the new, easier-to-use AML M7220 wireless handheld terminal will keep existing Terminal Emulation (TE) data collection applications running like new – and, at the right price for your budget.
» Learn more
OK

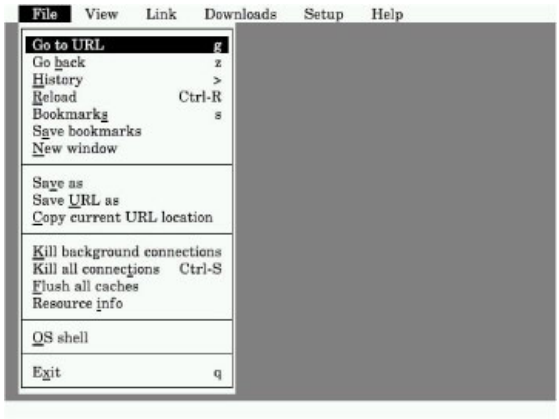
Text Mode

Google
Web Images Maps News Shopping Gmail more Dt
Video Groups Books Scholar Finance Blogs
YouTube Calendar Photos Documents Reader Sites
even more >>
iGoogle | Sign in
Google
[Google Search] [I'm Feeling Lucky]
Advertising Programs - Business Solutions - About Google
(c)2008 - Privacy
http://images.google.com/imghp?hl=en&tab=wi

Basic Usage

When browsing, Links2 displays a navigation bar at the top of the screen and a status bar at the bottom.

The navigation bar will show the current web page title on the right and give a "Back" button on the left. Tapping a blank area of the navigation bar will switch the bar to a normal File menu with all standard options and actions.

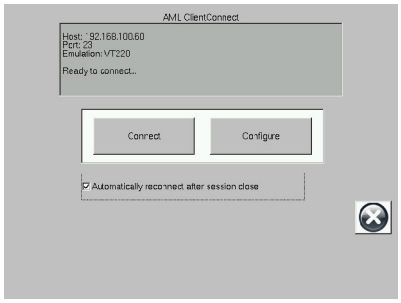


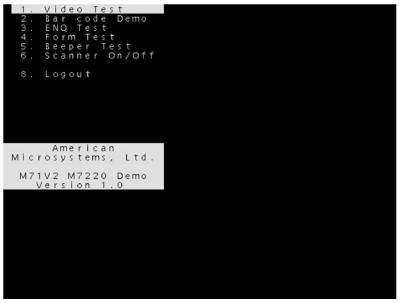
On-Screen Keyboard

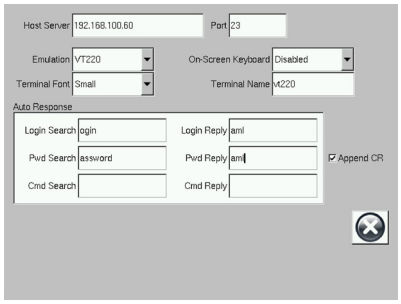
The unit includes a simple on-screen keyboard for use when no other input is available.

VT100/220 Terminal Emulator

The KDT750 contains a simple telnet client capable of emulating VT100 and VT220 terminals.







8

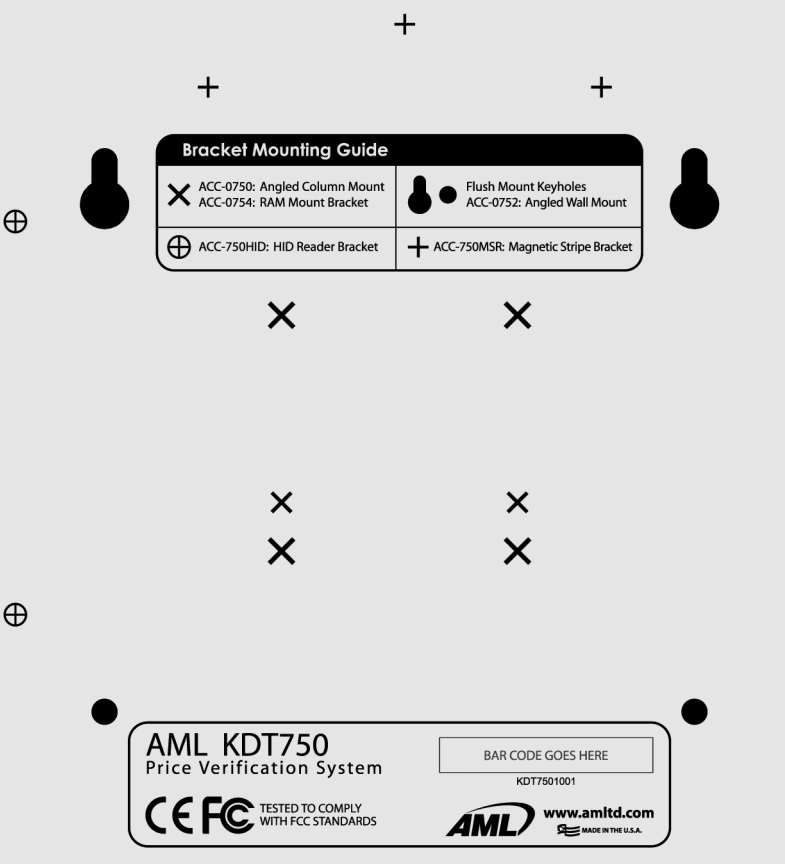
Mechanical Integration and Mounting

This chapter describes methods to mount the KDT750 unit in a variety of environments.

Rear Panel Mount Points

The KDT750 base unit is backed by a stainless steel rear panel with a variety of mounting patterns. Each pattern is indicated by the rear label. A sharp punch or knife can be used to punch through the label at the desired locations, and only the necessary holes should be knocked out to keep the unit environmentally sealed.

WARNING: THE REAR PANEL SHOULD BE REMOVED FROM THE OUTER CASE BEFORE PUNCHING ANY HOLES IN THE LABEL.

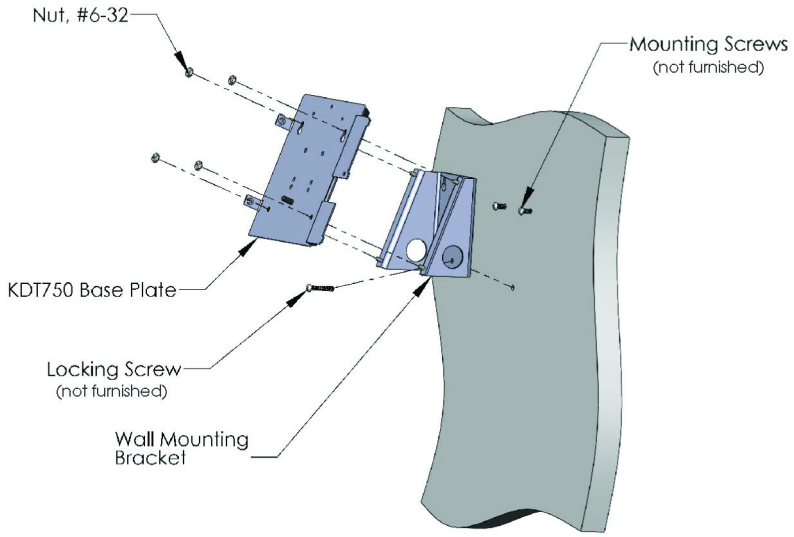


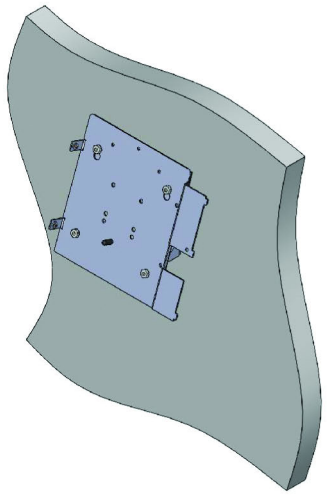
Flush Wall Mounting

The KDT750 base unit can be flush mounted with four screws via four holes in the rear panel (two "key-hole", two round). The rear panel's cable inlet is recessed, allowing for flush mounting in certain situations.

Angled Wall Mounting

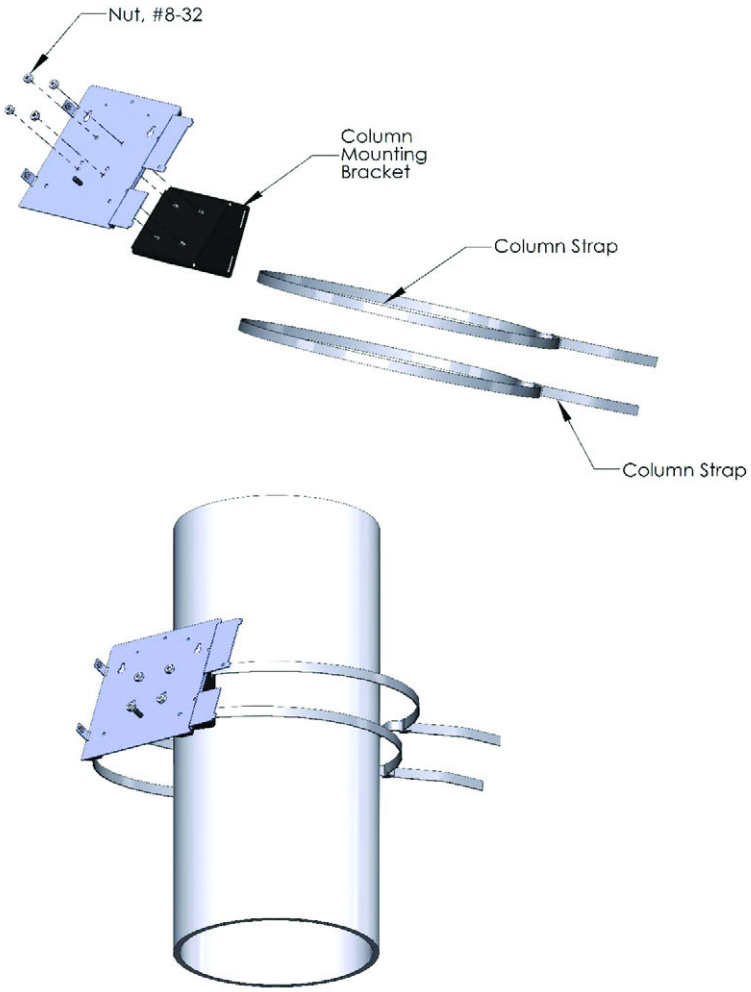
The optional Angled Wall Bracket (ACC-0752) hard mounts the KDT750 to any flat surface at a 20 degree angle, ideal for price checking applications. The bracket attaches to the KDT750's rear panel via four stainless steel studs and nuts.





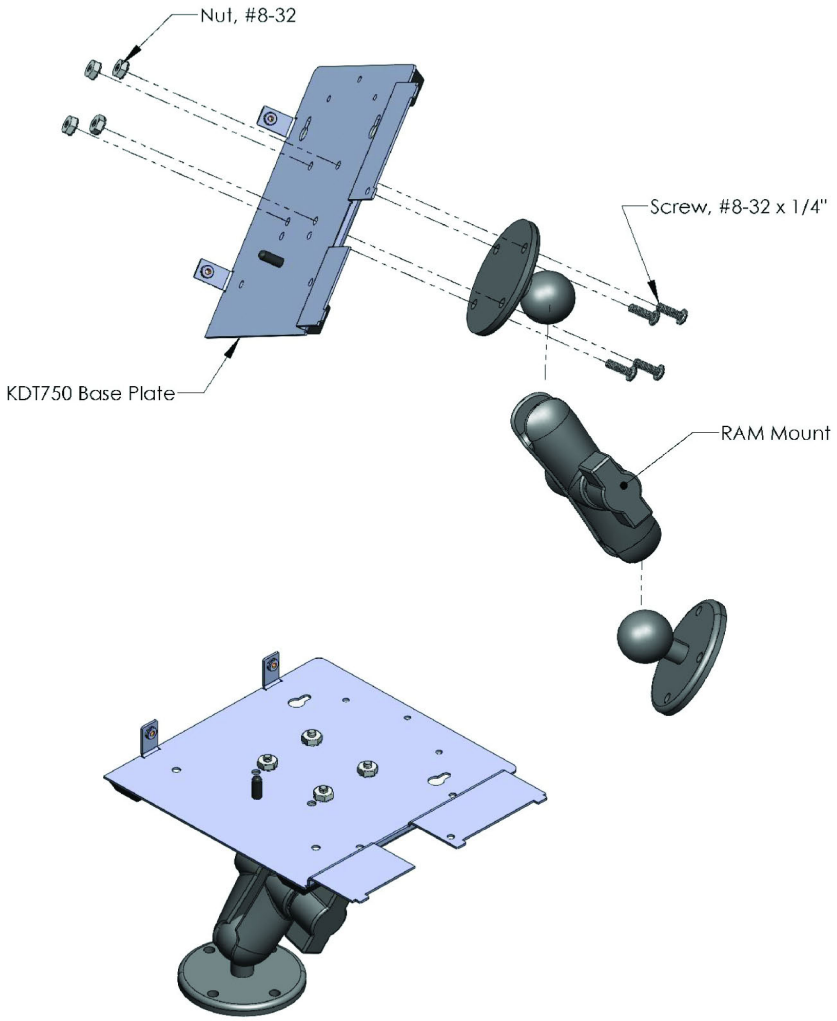
Column/Post Mounting

The KDT750 Pole Mount bracket (ACC-0750) is a non-destructive mounting solution for existing round structural or aesthetic posts and poles. By utilizing nylon or steel straps, the unit can be mounted to poles ranging in sizes from 4 to 24 inches in diameter. The ideal pole diameter for the bracket ranges from 6 to 16 inches.



RAM Mounts

The KDT750 can be mounted with the standard "B" size RAM® Mounting system. The rear panel of the base unit houses the standard 4 hole AMPS bolt pattern for attaching RAM ball and socket mounts. The RAM mounting system includes fully adjustable mounts, as well as locks, bases, accessory mounts and extensions.



Appendix A

Technical Specifications

General Specifications	
Dimensions	14.6 cm L x 7.2 cm W x 5.0 cm D(5.750" L x 6.625" W x 2.000" D)
Weight	0.81 lbs./363g
Display	5.6" VGA (640x480), 16-bit Color TFT LCD
Touchscreen	Integrated Resistive Touch Panel
Keypad	4 x Integrated momentary push-button
Power Supply	Power-over-Ethernet (48V, 802.3af Compliant) 12V DC 2.1 mm Barrel Jack
Internal UPS Battery	7.4V 2-Cell 2200 mAh Lithium-ion, ~1 hour runtime (Optional)
I/O Ports	3 x USB 1.1 Full Speed Host Ports 2 x RS-232 (1 x RJ-45, 1 x Expansion Header) 1 x Wiegand Interface (Header) 2 x Isolated Digital Inputs (Screw Terminal Block) 2 x Isolated Micro-Relay Outputs (Screw Terminal Block) 2 x Internal Bar Code Decoder Connector (12 & 14 Pin FPC Flex)
Networking	10/100Base-TX Fast Ethernet 802.11b/g/n Wireless Radio (Optional Internal USB Type)
Audio	Integrated Speaker and Amplifier (tonal)
Bar Code Decoding	Integrated Linear CCD Decoder (Optional) Integrated Omni-Directional, 2D (Optional)
Card Reading	Magnetic Stripe Reader (Optional) HID® ProxPoint® Proximity Card Reader (Optional)

Performance Specifications	
Processor	Samsung S3C2410 @ 202 MHz
Architecture	32-bit RISC ARM9 with AMBA (Advanced Microcontroller BusArchitecture)
Memory (RAM)	64 MB 100MHz SDRAM
Memory (Flash storage)	1024 MB (1 GB) Storage (SD Card) 16 MB Integrated Flash ROM (Operating System)
Memory Expansion	1 GB SD Card Included
Operating System	Linux (AML GNU/Linux, Kernel 2.6.22)

Environmental Specifications	
Operating Temperature	-20° to 50° C / -4° to 122° F
Storage Temperature	-30° to 60° C / -30° to 140° F
Humidity	0% to 90% RH, non-condensing
Electrostatic Discharge	15kVDC through air 8kVDC contact
Sealing	IP54 NEMA 12

Regulatory Specifications	
Certifications	FCC, CE
Environmental	RoHS, Pb-Free

Optional Wireless Radio Specifications	
Radio	IEEE 802.11n Draft v2.0; IEEE 802.11b; IEEE 802.11g
Frequency	2.4 GHz Range
Signal Rates	11n (40MHz): up to 300Mbps; 11n (20MHz): up to 144Mbps; 11g: up to 54Mbps; 11b: up to 11Mbps
Output Power	802.11b: 17± 1dBm 802.11g: 17± 1dBm 802.11n: 15± 1dBm
Antenna Configuration	1T2R Internal Antenna (1 Transmit / 2 Receiving)
Receive Sensitivity	802.11g: -70dBm @54Mbps 802.11b: -83dBm @11Mbps 802.11n: -83dBm @11Mbps
Security	None 64/128 Bit WEP WPA/WPA2 Personal (PSK) WPA/WPA2 Enterprise (EAP) 802.1x Authentication Supplicants

Appendix B

Wireless Reference Table

Wireless Reference Table		
WEP	Remote Authentication Dial In User Service	WEP was initially intended to provide a level of confidentiality on a wireless network that was comparable to a wired infrastructure. WEP does not allow for any true authorization (only encryption) and does not protect users or devices from each other on the network. There are two main WEP types: WEP Open System (Standard WEP) – All data transmissions are encrypted with the WEP key. No attempt is made to authorize the client device. WEP Shared Key – In Shared Key, a very insecure attempt to authorize the device is attempted. The actual WEP encryption key is sent to the host (usually the access point) to verify the identity of the device. This exposes the enciphering key to the network, and should not be used. In a WEP enabled environment, each client holds the common network encryption keys which can be either a 40-bit key for 64-bit encryption or a 104-bit key for 128-bit encryption. These keys are common to all devices on the network and are used to encrypt all data transmissions. Because each network packet is encrypted with the same key, and because of flaws in the actual cipher, WEP is no longer considered secure, and an attacker, depending on network traffic, could determine the network encryption keys by eavesdropping on the transmissions. It has been demonstrated in a controlled environment that these attacks can take as little as 10 minutes to determine a 40-bit key.
WPA	Wifi Protected Access	WPA was created in response to the weaknesses of WEP, and while it implements the majority of the IEEE 802.11i standard, it is not considered to be fully compliant. WPA was only intended as a temporary measure to be used in place of WEP while the final 802.11i standard was being drafted. WPA was designed to work on all existing 802.11 hardware to provide a considerable amount of protection compared to WEP. WPA was designed for use with an 802.1x (commonly referred to as RADIUS) server to provide authentication and to distribute encryption keys to the clients. It is possible, however, to use WPA in "Personal" Pre-shared key (PSK) mode which allows the benefits of WPA without the need of the external 802.1x server, but this is

Wireless Reference Table		
		considered to be less secure. Each client in a PSK environment holds a common passphrase that is used to generate the keys. Weak passphrases is the major concern when using PSK. One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. The more often that the encryption key changes, the less data a potential attacker can get on the key, and, even if they were to determine the current key, once a new key was rotated in, they would de-authenticated again. WPA also defined the use of EAP for authentication of users, however it does not define all of the EAP types that are employed in WPA2.
WPA2	Wifi Protected Access Version 2	WPA2 contains the following components: 802.1x for authentication (entailing the use of EAP and an authentication server), RSN (Robust Security Network) for keeping track of associations, and AES-based CCMP encryption to provide confidentiality, integrity and origin authentication. The CCMP algorithm is the heart of WPA2 and is what sets it apart from WPA. CCMP was designed to replace both TKIP and WEP, and handles message integrity, encryption and authentication. Most, if not all of the capabilities of WPA can be implemented in WPA2 with CCMP, which is considered the state of the art.
802.11i	IEEE 802.11i Standard	The IEEE standard. Commonly called WPA2.
TKIP	Temporal Key Integrity Protocol	Dynamic key rotation algorithm often used in WPA environments.
CCMP (AES)	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	Encipherment algorithm designed to replace TKIP and WEP in WPA2/802.11i. CCMP is considered state of the art.
EAP	Extensible Authentication Protocol	EAP is a general authentication method that can be used in many technologies, but it is most commonly found in wireless LANs. A large amount of documentation refers to WPA-EAP as "WPA Enterprise" even though it is an ambiguous term. There are many subtypes of EAP, but only five have been described as standard. The MT7570 supports the following EAP types for authentication. EAP-TLS – EAP Transport Layer Security is the original standard wireless LAN EAP authentication protocol. Although it is rarely deployed, it is still considered one of the most secure EAP standards available and

Wireless Reference Table

		the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off. EAP-TTLS - Tunneled Transport Layer Security was co-developed by Funk Software and Certicom and is widely supported across platforms. It was never fully ratified, only drafted (the draft which has since expired), but is still common due to its decent level of security and easy setup. EAP-PEAP - Protected Extensible Authentication Protocol is widely available in products, and provides very decent authentication security. Its method is similar in design to EAP-TTLS but requires only a server-side certificate to create a secure tunnel to protect user authentication. PEAPv0/EAP-MSCHAPv2 is what most are referring to when the term "PEAP" is used. Behind EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world. EAP-LEAP - The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems, Inc. It is considered less secure than other EAP types, even by Cisco, and is not recommended in new installations.
PSK	Pre-shared Key	Often called "WPA/WPA2 Personal", PSK allows the use of common passphrases for authentication. PSK is often used in smaller networks that wish to use the high security of WPA/WPA2 but do not wish to employ an 802.1x authentication server.
802.1x	IEEE 802.1X	IEEE Standard for authentication. Often in wireless documentation, references to"802.1x" are really meaning 802.1x Authentication Server or RADIUS server that provides authentication and encryption keys to the clients.
RADIUS	Remote Authentication Dial In User Service	Often, administrators will call the 802.1x server the "RADIUS" server. RADIUS is an authentication, authorization, and accounting protocol for applications such as network access or IP mobility. In the wireless LAN environment, RADIUS is commonly used to implement the 802.1x standard.